## CLAIMS

What is claimed is:

1. A random number generator comprising:

a computer having a parallel port, said parallel port including data and control lines;

a random number generator circuit for producing a random sequence of signals, said random number generator circuit including power supply means for powering said circuit from power supplied by one or more of the data and control lines of said parallel port; and

electrical connecting means for transferring power from said computer to said power supply means via said parallel port and for communicated signals generated by said random number generator circuit to said computer through said parallel port.

2. A random number generator as in claim 1 wherein said power supply means comprises a charge pump.

3. A random number generator as in claim 1 wherein said computer includes device driver means for operating said random number generator circuit through said parallel port.

4. A random number generator as in claim 1 wherein said random number generator circuit includes a source of true random signals, said source being selected from the group consisting of: a thermal noise source; and an intrinsically random quantum source.

5. A random number generator system comprising:

a computer including a power source producing a first voltage of one sign;

a charge pump for producing a second voltage of the opposite sign to said first voltage; and

a random number generator circuit powered by said first and second voltages for generating a random sequence of signals.

6. A random number generator as in claim 5 wherein said first voltage is a positive voltage and said second voltage is a negative voltage.

7. A random number generator as in claim 5 wherein said charge pump comprises an analog multiplexer circuit.

8. A random number generator comprising a circuit for generating a sequence of binary signals, and a computer for receiving said binary signals and utilizing them, said circuit using 30 milliwatts of power or less.

9. A random number generator as in claim 8 wherein said circuit comprises:

an analog noise generator for producing an analog noise signal; and

a comparator, responsive to said analog noise signal, for providing said sequence of binary signals, said comparator: having a rise time up to 25 nanoseconds, drawing less than three milliamps of current, and operating down to 2 volts.

10. A random number generator as in claim 9 wherein said comparator means comprises a XHCU04 hex inverter, where X is 54 or 74.

11. A random number generator circuit comprising: an analog noise generator; a charge pump for providing a voltage to said analog noise generator, an analog to binary converter for converting said analog noise to a binary signal, a randomness defect reducer for reducing randomness defects in said binary signal, and a buffer for driving said signal to an electronic device external of said random number generator circuit.

12. A random number generator circuit as in claim 11 wherein each of said charge pump, said analog noise generator, said analog to binary converter, said randomness defect reducer, and said buffer include a separately filtered power supply.

13. A random number generator circuit as in claim 11 wherein each of said charge pump, said analog noise generator, said analog to binary converter, said randomness defect reducer, and said buffer comprise a CMOS integrated circuit.

14. A random number generator circuit as in claim 11 wherein the total current used by said charge pump, said analog noise generator, said analog to binary converter, said randomness defect reducer, and said buffer is 8 milliamps or less.

15. A random number circuit for producing a sequence of binary signals, said circuit comprising:

a source of a white noise electrical signal; and amplifier means for amplifying said white noise signal while adding an amplifier noise signal to said white noise signal; and

wherein said amplifier noise is one-third or less of the total noise signal comprising said white noise signal and said amplifier noise signal.

16. A random number generator as in claim 15 wherein said circuit further includes high pass filter means for removing a low-frequency tail in said total noise signal, said high pass filter means having a cut-off frequency in the range from 36 Hertz to 170 Hertz.

17. A random number generator as in claim 16 wherein said total noise signal has a bandwidth of from 100 Hz to 100 KHz and is flat within ±0.25 db over said bandwidth.

18. A random number generator circuit for proving a sequence of binary signals, said circuit comprising:

an analog noise generator for producing an analog noise signal; and

comparator means, responsive to said analog noise signal, for providing said sequence of binary signals, said comparator means comprising an XHCU04 hex inverter, where X is 54 or 74.

19. A random number generator circuit comprising:

a source of a white noise electrical signal; and

amplifier means for amplifying said white noise signal, said amplifier means comprising one or more operational amplifiers selected from the group consisting of: TL06X operational amplifiers, where X is 0, 1, 2, or 4, LF44Y operational amplifiers, where Y is 1, 2, or 4, and AD548 and AD648 single and dual operational amplifiers.

20. A random number generator circuit comprising: a low amplitude circuit portion; a normal amplitude circuit portion; and an EMI shield enclosing said low amplitude circuit portion, wherein said low amplitude circuit portion is mounted on a printed circuit board and said shield comprises: a ground plane on said circuit board located around said low amplitude circuit portion in the plane of said circuit board, a component side cover and a solder side cover, said covers electrically connected to said ground plane.

21. A random number generator comprising:

a random number generator circuit for generating a random sequence of signals; and

a computer including a means for interfacing with said random number generator circuit, said means for interfacing consisting of one or more of the following: a device driver, a TSR, a portion of the operating system of said computer, and a program stored in the bios memory of said computer.

22. A random number generator as in claim 21 wherein said means for interfacing comprises a device driver.

23. A random number generator as in claim 21 wherein said means for interfacing comprises software for testing said random number generator circuit.

24. A random number generator as in claim 21 wherein said random number generator circuit is located in a module separate from said computer, and said random number generator further includes a cable for electrically connecting said module to said computer.

25. A random number generator as in claim 21 wherein said random number generator circuit is located on an add-on board for mounting in said computer.

26. A random number generator as in claim 21 wherein said random number generator circuit is located on the motherboard of said computer.

27. A random number generator as in claim 21 wherein said random number generator circuit is located on a peripheral of said computer.

28. A device for interfacing with a random number generator, said device comprising:

a computer including: memory means for storing information for interfacing with a random number generator circuit, and processing means communicating with said memory for interfacing with said random number generator; and wherein

said information for interfacing with a random number generator consists of one or more of the following: a device driver, a TSR, a portion of the operating system of said computer, and a program stored in the bios memory of said computer.

29. A random number generator comprising:

a circuit for producing a sequence of binary signals; and sample means for sampling said sequence of binary signals at a sampling rate between 50% and 125% of the sampling rate at the knee on the serial dependence versus delay time curve describing said circuit to provide a random sequence of signals at said sampling rate.

30. A random number generator as in claim 29 wherein said sampling rate is at the knee of said serial dependence versus delay time curve.

31. A random number generator as in claim 29 and further including randomness defect reducer means for reducing the randomness defects in said sequence of binary signals.

32. A random number generator as in claim 31 wherein said randomness defect reducer means comprises a component selected from the group consisting of an EXCLUSIVE OR gate and a divider.

33. A method of generating a random sequence of signals, said method comprising the steps of:

providing a circuit for producing a sequence of signals; and

sampling said sequence of signals at a sampling rate between 50% and 125% of a sampling rate corresponding to the knee on the serial dependence versus delay time curve describing said circuit to provide a random sequence of signals at said sampling rate.

34. A method as in claim 33 wherein said step of sampling comprises measuring a statistical parameter as a function of a time parameter related to the delay time of said random sequence of signals, said function having a knee where the character of said function changes from being essentially related to statistics to being essentially related to real physical characteristics of said circuit; and sampling said random sequence of signals at a sampling rate corresponding to a point on said function between 50% and 125% of the sampling rate at said knee to generate said random sequence of signals.

35. A method of designing and fabricating a random number generator, said method comprising the steps of:

designing and making a circuit for producing a binary random sequence of signals;

measuring a first parameter of said binary sequence of signals, said parameter related to the serial dependence of said binary random sequence;

calculating the degree of defects in randomness in said sequence for one or more levels of defect correction to determine the optimum number of levels of defect correction to produce a random number generator with a desired randomness quality; and

fabricating a random number generator comprising said circuit and said optimum number of levels of defect correction.

36. A method as in claim 35 wherein:

said step of calculating comprises calculating said degree of defects in randomness as a function of a second parameter related to the delay time to determine the said optimum number of levels for different values of said second parameter; and

said step of fabricating comprises fabricating a random number generator having an optimum number of levels for a selected delay time.

37. A method as in claim 36 wherein said first parameter comprises one or more parameters selected from the group consisting of $B_2$ and SD(t) and said second parameter comprises a parameter selected from the group consisting of delay time and sample rate.

38. A method as in claim 35 wherein said step of fabricating includes providing at least one level of defect correction comprising EXCLUSIVE OR gate means for combining pairs of consecutive binary signals in said sequence of signals.

39. A method as in claim 35 wherein said step of fabricating includes providing at least one level of defect correction comprising a divider.

40. A method of generating a sequence of random numbers, said method comprising the steps of:

providing a circuit for producing a binary random sequence of signals;

measuring a parameter of said binary sequence of signals, said parameter related to the serial dependence of said binary random sequence;

~~calculating the degree of defects in randomness in said sequence for one or more levels of defect correction to determine the optimum number of levels of defect correction for a desired randomness quality; and~~

~~reducing the defects in said binary random sequence of signals by providing said optimum number of levels of defect correction.~~

add a2 >

add B1 >